


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
**Search:**  The ACM Digital Library  The Guide

elliptic curve binary series hidden point



Searching within **The ACM Digital Library** for: elliptic curve binary series hidden point ([start a new search](#))  
 Found 16 of 264,269

**REFINE YOUR SEARCH**
**▼ Refine by Keywords**

elliptic curve binary se



Discovered Terms

**▼ Refine by People**

Names

Institutions

Authors

Editors

Reviewers

**▼ Refine by Publications**

Publication Year

Publication Names

ACM Publications

All Publications

Content Formats

Publishers

**▼ Refine by Conferences**

Sponsors

Events

Proceeding Series

**ADVANCED SEARCH**
[Advanced Search](#)
**FEEDBACK**

A small icon of a speech bubble with a checkmark inside.
 Please provide us with feedback

Found 16 of 264,269

**Search Results**

Results 1 - 16 of 16

**Related Journals**
**Related Magazines**
**Related SI**

Sort by

A small icon of a binder with a checkmark inside.
 Save results to a Binder

**1 Communications of the ACM: Volume 51 Issue 1**

A small icon of a journal page with a checkmark inside.
 January 2008 Communications of the ACM

**Publisher:** ACM

 Full text available: Digital Edition , Pdf (5.97 MB) Additional Information: [full citation](#), [abs](#)
**Bibliometrics:** Downloads (6 Weeks): 673, Downloads (12 Months): 3166, Dov

**2 Side-channel resistant system-level design flow for public-key crypto**

A small icon of a conference banner with a checkmark inside.
 Kazuo Sakiyama, Elke De Mulder, Bart Preneel, Ingrid Verbauwhede

**March 2007 GLSVLSI '07: Proceedings of the 17th ACM Great Lakes sym**
**Publisher:** ACM 

 Full text available: Pdf (650.57 KB) Additional Information: [full citation](#), [abs](#)
**Bibliometrics:** Downloads (6 Weeks): 7, Downloads (12 Months): 42, Dov

In this paper, we propose a new design methodology to assess the risk timing analysis and simple power analysis, at an early design stage. This elliptic curve cryptographic ...

**Keywords:** elliptic curve cryptography, side-channel attack, system-lev

**3 Reconfigurable computing: a survey of systems and software**

A small icon of a conference banner with a checkmark inside.
 Katherine Compton, Scott Hauck

**June 2002 Computing Surveys (CSUR)** , Volume 34 Issue 2

**Publisher:** ACM 

 Full text available: Pdf (710.56 KB) Additional Information: [full citation](#), [abs](#)
**Bibliometrics:** Downloads (6 Weeks): 122, Downloads (12 Months): 883, Dov

Due to its potential to greatly accelerate a wide variety of applications, subject of a great deal of research. Its key feature is the ability to perform reconfiguration, while retaining ...

**Keywords:** Automatic design, FPGA, field-programmable, manual desi, reconfigurable computing, reconfigurable systems

**4 A survey of RFID privacy approaches**

Marc Langheinrich

**August 2009 Personal and Ubiquitous Computing** , Volume 13 Issue 6

**Publisher:** Springer-Verlag

Full text available: Pdf (308.39 KB)

Additional Information: full citation, abstract

**Bibliometrics:** Downloads (6 Weeks): 220, Downloads (12 Months): 350, Download Link

A bewildering number of proposals have offered solutions to the privacy problem. This article tries to give an overview of the currently discussed approaches.

**Keywords:** Privacy, RFID

**5 On the power of simple branch prediction analysis**

Onur Acilmez, Cetin Kaya Koç, Jean-Pierre Seifert

March 2007 **ASIACCS '07: Proceedings of the 2nd ACM symposium on Information security and privacy**

**Publisher:** ACM

Full text available: Pdf (3.40 MB)

Additional Information: full citation, abstract

**Bibliometrics:** Downloads (6 Weeks): 16, Downloads (12 Months): 95, Download Link

Very recently, a new software side-channel attack, called Branch Predictor attack, was discovered and also demonstrated to be practically feasible on popular microprocessors. This recent attack still had the flavor ...

**Keywords:** RSA, branch prediction analysis, modular exponentiation, side-channel attacks

**6 MAX: Wide area human-centric search of the physical world**

Kok-Kiong Yap, Vikram Srinivasan, Mehul Motani

August 2008 **Transactions on Sensor Networks (TOSN)**, Volume 4 Issue 4

**Publisher:** ACM

Full text available: Pdf (6.03 MB)

Additional Information: full citation, abstract

**Bibliometrics:** Downloads (6 Weeks): 22, Downloads (12 Months): 203, Download Link

We propose MAX, a system that facilitates human-centric search of the physical world. A priori, it allows humans to search for and locate them as needed. Describes the system's architecture and its human-centric operation, ...

**Keywords:** Human-centric, landmark-based localization, physical world

**7 Proceedings of the 2005 ACM symposium on Applied computing**

Hisham M. Haddad, Andrea Omicini, Roger L. Wainwright, Lorrie M. Liebrock

March 2005 **SAC '05: Proceedings of the 2005 ACM symposium on Applied computing**

**Publisher:** ACM

Additional Information: full citation, abstract

**Bibliometrics:** Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Download Link

Welcome to the 20th Annual ACM Symposium on Applied Computing (SAC). We are in Socorro, New Mexico, USA. As the Conference Chair, thank you for participating ...

**8**

Level set and PDE methods for computer graphics

David Breen, Ron Fedkiw, Ken Museth, Stanley Osher, Guillermo Sapiro, Et August 2004 SI GGRAPH '04: SIGGRAPH 2004 Course Notes

**Publisher:** ACM Request Permissions

Full text available: Pdf (17.07 MB)

Additional Information: [full citation](#), [absi](#)

**Bibliometrics:** Downloads (6 Weeks): 131, Downloads (12 Months): 1050, Dov

Level set methods, an important class of partial differential equation (PDE) implicitly as the level set (iso-surface) of a sampled, evolving nD function that introduces the ...

**9 The elements of nature: interactive and realistic techniques**

Oliver Deussen, David S. Ebert, Ron Fedkiw, E. Kenton Musgrave, Przemyslaw Tessendorf

August 2004 SI GGRAPH '04: SIGGRAPH 2004 Course Notes

**Publisher:** ACM Request Permissions

Full text available: Pdf (17.65 MB)

Additional Information: [full citation](#), [absi](#)

**Bibliometrics:** Downloads (6 Weeks): 220, Downloads (12 Months): 1551, Dov

This updated course on simulating natural phenomena will cover the latest in simulating most of the elements of nature. The presenters will provide research perspectives ...

**10 GPGPU: general purpose computation on graphics hardware**

David Luebke, Mark Harris, Jens Krüger, Tim Purcell, Naga Govindaraju, Ia

August 2004 SI GGRAPH '04: SIGGRAPH 2004 Course Notes

**Publisher:** ACM Request Permissions

Full text available: Pdf (63.03 MB)

Additional Information: [full citation](#), [absi](#)

**Bibliometrics:** Downloads (6 Weeks): 244, Downloads (12 Months): 1625, Dov

The graphics processor (GPU) on today's commodity video cards has evolved significantly. The latest graphics architectures provide tremendous memory bandwidth with fully programmable vertex ...

**11 Design, implementation and testing of extended and mixed precision**

Xiaoye S. Li, James W. Demmel, David H. Bailey, Greg Henry, Yozo Hida, J

Anil Kapur, Michael C. Martin, Brandon J. Thompson, Teresa Tung, Daniel A.

June 2002 Transactions on Mathematical Software (TOMS), Volume 28, Number 4

**Publisher:** ACM Request Permissions

Full text available: Pdf (456.84 KB)

Additional Information: [full citation](#), [absi](#)

**Bibliometrics:** Downloads (6 Weeks): 10, Downloads (12 Months): 87, Dov

This article describes the design rationale, a C implementation, and a Fortran Standard for the BLAS (Basic Linear Algebra Subroutines): Extended and mixed precision arithmetic ...

**Keywords:** BLAS, double-double arithmetic, extended and mixed precision

**12 A review of vessel extraction techniques and algorithms**

Cemil Kirbas, Francis Quek

June 2004

**Computing Surveys (CSUR)** . Volume 36 Issue 2 Publisher: ACM Request PermissionsFull text available:  Pdf (8.06 MB)Additional Information: [full citation](#), [abs](#)**Bibliometrics:** Downloads (6 Weeks): 89, Downloads (12 Months): 699, Download

Vessel segmentation algorithms are the critical components of circulatory systems. In this paper we present a survey of vessel extraction techniques and algorithms. We put the various techniques in perspective ...

**Keywords:** Magnetic resonance angiography, X-ray angiography, medical image processing, vessel segmentation**13 The data mining approach to automated software testing** Mark Last, Menahem Friedman, Abraham Kandel August 2003 **KDD '03: Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining** Publisher: ACM Request PermissionsFull text available:  Pdf (296.40 KB)Additional Information: [full citation](#), [abs](#)**Bibliometrics:** Downloads (6 Weeks): 53, Downloads (12 Months): 338, Download

In today's industry, the design of software tests is mostly based on the test cases. These test cases are limited to execution of pre-planned tests only. Evaluation of test output by human ...

**Keywords:** automated software testing, finite element solver, info-fuzz testing**14 A system for understanding imaged infographics and its applications** Weihua Huang, Chew Lim Tan August 2007 **DocEng '07: Proceedings of the 2007 ACM symposium on Document engineering** Publisher: ACM Request PermissionsFull text available:  Pdf (1.13 MB)Additional Information: [full citation](#), [abs](#)**Bibliometrics:** Downloads (6 Weeks): 14, Downloads (12 Months): 59, Download

Information graphics, or infographics, are visual representations of information. The study of infographics in documents is a relatively new research problem, which has been studied by several researchers. Infographics can appear as raster images, vector images, or as a combination of both ...

**Keywords:** applications, association of text and graphics, document imaging, infographics**15 Artistic screening** Victor Ostromoukhov, Roger D. Hersch September 1995 **SIGGRAPH '95: Proceedings of the 22nd annual conference on Computer graphics and interactive techniques** Publisher: ACM Request PermissionsFull text available:  Pdf (4.15 MB)Additional Information: [full citation](#), [abs](#)**Bibliometrics:** Downloads (6 Weeks): 6, Downloads (12 Months): 44, Download

**Keywords:** artistic screening, graphic design, halftoning, image reprod

**16 Shrouds: optimal separating surfaces for enumerated volumes**

Gregory M. Nielson, Gary Gral, Ryan Holmes, Adam Huang, Mariano Phelip  
May 2003    **VISSYM '03: Proceedings of the symposium on Data visualis**

**Publisher:** Eurographics Association

Full text available:  Pdf (1.58 MB)

Additional Information: [full citation](#), [abs!](#)

**Bibliometrics:** Downloads (6 Weeks): 1,   Downloads (12 Months): 8,   Download

We describe new techniques for computing a smooth triangular mesh surface consisting of a collection of points from a 3D rectilinear grid. The surface is generated by a marching cubes ...

The ACM Portal is published by the Association for Computing Machinery. Copyright ©  
[Terms of Usage](#)   [Privacy Policy](#)   [Code of Ethics](#)   [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)    [QuickTime](#)    [Windows Media Player](#)